RA Mag. Michael Pilz, Wien

Datenschutz und Arbeitsrecht – eine Beeinflussung

Übersicht:

9783214042479
Digitale Arbeitswelt
Wolfgang Kozak
MANZ Verlag Wien

I. Einleitung

Der gegenständliche Beitrag befasst sich mit den Interdependenzen zwischen Arbeitsrecht und Datenschutzrecht. Die zunehmende Bedeutung datenschutzrechtlicher Fragestellungen seit dem Inkrafttreten der Datenschutz-Grundverordnung der Europäischen Union (DSGVO) im Mai 2018 hat auch dazu geführt, dass arbeitsrechtliche Auseinandersetzungen vermehrt auf der Ebene des Datenschutzes ausgetragen werden. Für Arbeitgeber:innen und Arbeitnehmer:innen werden datenschutzrechtliche Fragestellungen auch zu einem Instrument, um nicht nur die Konformität mit datenschutzrechtlichen Grundsätzen zu erzwingen, sondern auch, um möglicherweise dahinter liegende Interessen in der antagonistischen Auseinandersetzung mit dem Gegenüber durchzusetzen.

In der arbeitsrechtlichen Praxis wird daher eine Beschäftigung mit datenschutzrechtlichen Fragen immer wichtiger; nicht nur bei der Beurteilung behaupteter arbeitsrechtlicher Verfehlungen im Rahmen von Kündigungsanfechtungen oder Entlassungsprozessen, sondern auch bei der Einordnung von rechtlichen Möglichkeiten und Instrumenten in Zusammenhang mit der Speicherung von Arbeitnehmer:innendaten durch die Arbeitgeber:innen, den datenschutzrechtlichen Aspekten von Überwachungsmaßnahmen im Betrieb und den Möglichkeiten des Einsatzes der datenschutzrechtlichen Kontrollinstrumente zur Sanktionierung unerwünschter Verhaltensweisen des jeweiligen Gegenübers.

Sie finden im Folgenden daher eine Auswahl datenschutzrechtlicher Fälle und Entscheidungen zur interessierten Lektüre, zur Einführung in datenschutzrechtliche Fragestellungen insbesondere für Praktiker:innen des Arbeitsrechts und zur Anregung für die weitere Ausweitung möglicher Instrumente in arbeitsrechtlichen Auseinandersetzungen.

II. Aktuelle Fallbeispiele und Entscheidungen

Im folgenden Kapitel werden eine Reihe von Rechtsfällen aus der anwaltlichen Praxis vorgestellt und analysiert, welche das aufgrund der voranschreitenden **Digitalisierung** immer wichtiger werdende **Zusammenspiel von Datenschutz- und Arbeitsrecht** aufzeigen sollen. Teilweise handelt es sich um bereits von den zuständigen Behörden entschiedene Fälle, teilweise werden auch anhängige Verfahren dargestellt, weil diese besonders illustrativ für den Themenkomplex Datenschutz/Arbeitsrecht sind. Bei der Auswahl wird den geneigten Leser:innen auffallen, dass nicht nur die Arbeitgeber:innen, welche naturgemäß eine Fülle an Daten über die Arbeitnehmer:innen verarbeiten, Gegenstand von Verfahren vor der Datenschutzbehörde sind, sondern auch die Organe der Arbeitnehmer:innenschaft – auch diese sind dazu verpflichtet, die Vorgaben der DSGVO und des DSG einzuhalten und die ihnen zur Verfügung gestellten Daten nur im zulässigen Rahmen zu verarbeiten.

A. Emailscan

1. Sachverhalt

Aus einem größeren Unternehmen wurde offenbar das **Protokoll einer Aufsichtsratssitzung** an ein **Medium weitergegeben,** um die Berichterstattung über einen angeblichen Missstand zu ermöglichen. Nachdem die geleakten Protokolle – teilweise wörtlich – in dem Medium veröffentlicht wurden, erteilte die Unternehmensleitung den **Auftrag,** die **Emailkonten** aller Mitarbeiter:innen (insgesamt 6.000 Personen) auf eine etwaige Korrespondenz mit dem Medium **zu durchsuchen**. Die angeordnete Kontrolle beschränkte sich dabei auf die technischen Mail-Serverprotokolle **(Logfiles),** ohne dass Inhalte durchsucht wurden. Insgesamt wurden die Emailkonten von rund 6.000 Mitarbeiter:innen darauf durchsucht, ob von ihnen ausgehend ein Email an die Redaktion des veröffentlichenden Mediums geschickt worden war, obwohl lediglich 26 Mitarbeiter:innen tatsächlich Zugriff auf das Protokoll hatten. Gemäß einer abgeschlossenen Betriebsvereinbarung war auch eine **private Nutzung** der Arbeitsemailadressen **zulässig,** weshalb die Durchsuchung einen besonders schweren Eingriff in die Privatsphäre der Betroffenen bedeutete. Die Durchsuchung führte zu keinem Treffer.

2. Rechtliche Beurteilung

Die Beschwerdeführer:innen, allesamt **Dienstnehmer:innen** des Unternehmens, dessen Emails durchsucht wurden, machten vor der Datenschutzbehörde (DSB) eine **Verletzung ihres Rechts auf Geheimhaltung** (§ 1 DSG) geltend – jede Person hat ein Recht auf Geheimhaltung ihrer personenbezogenen Daten, soweit daran ein schutzwürdiges Interesse besteht. Bei der **Auslegung** des Bedeutungsgehalts des Rechts auf Geheimhaltung sind die **DSGVO** und insbesondere die darin verankerten Grundsätze zu beachten.[1]) Ohne Probleme war die Frage zu bejahen, ob es sich bei den Logfiles um **personenbezogene Daten** iSd Art 4 Z 1 DSGVO handelt: Jedes Email ist mit einer Emailadresse der Absender:in bzw der Empfänger:in verbunden, die Log-Files beziehen sich somit auf eine identifizierbare Person.

Beim Grundrecht auf Geheimhaltung handelt es sich um ein **Grundrecht mit unmittelbarer Drittwirkung.**[2]) Somit ist nicht nur der Staat zur Geheimhaltung schützenswerter Daten verpflichtet, sondern sind dies auch **sämtliche Privatpersonen** (so auch die Arbeitgeber:innen). Sofern ein berechtigtes Interesse gem Art 6 Abs 1 lit f DSGVO iVm § 1 Abs 2 DSG an der Verarbeitung der personenbezogenen Daten besteht, ist eine **Interessensabwägung** durchzuführen.

Im vorliegenden Fall wurde von der Arbeitgeberin die Verhinderung zukünftiger Verletzungen von Betriebsgeheimnissen durch Veröffentlichung vertraulicher Sitzungsprotokolle als berechtigtes Interesse vorgebracht. Im Rahmen der Interessensabwägung wurde weiter argumentiert, dass einerseits nur Logfiles und keine inhaltlichen Daten verarbeitet worden waren und andererseits der

[1]) DSB 31. 10. 2018, DSB-D123.076/0003-DSB/2018; Newsletter der DSB 1/2023, S 5.

[2]) *Thiele/Wagner*, Praxiskommentar zum Datenschutzgesetz (DSG)[2] (2022) § 1 Rz 38.

Zentralbetriebsrat miteinbezogen worden sei. Somit sei ohnehin das gelindeste Mittel gewählt worden, um das Ziel zu erreichen.

Auf Seiten der Beschwerdeführer:innen wurde dem entgegnet, dass das Unternehmen die Maßnahme erst sechs Monate nachdem die Medienberichterstattung erfolgt war, durchführte, was ein geringes Interesse an der Rechtsverletzung indiziere. Ebenso hätte eine Einschränkung der durchsuchten Personen oder Arbeitsgruppen stattfinden müssen, eine pauschale Durchsuchung von 6.000 Emailkonten sei als überschießend und somit unverhältnismäßig zu beurteilen. Ergänzend wurde eingewandt, dass eine Zustimmung des Betriebsrats einzuholen gewesen wäre[3]), was jedoch unterblieb. Lediglich der (unzuständige) Zentralbetriebsrat war beratend einbezogen worden.

Die **Datenschutzbehörde folgte der Argumentation** der Beschwerdeführer:innen und erklärte die durchgeführten Kontrollmaßnahmen, insbesondere aufgrund vorliegender Unverhältnismäßigkeit[4]), für **rechtswidrig.**[5])

Aus der Entscheidung lässt sich herausarbeiten, dass den Arbeitgeber:innen bei der Durchsuchung der Emailadressen der Arbeitnehmer:innen **enge Grenzen gesetzt** sind. **Bereits die Abfrage von Logfiles bedarf einer ausgewogenen Verhältnismäßigkeitsprüfung.** Die Einbindung des (zuständigen) Betriebsrats kann dabei im Rahmen der Interessensabwägung zu Gunsten der Arbeitgeber:in gewertet werden.[6]) **Offen geblieben** ist die Frage, ob bzw unter welchen Voraussetzungen eine **inhaltliche Analyse** der Emailkonten der Dienstnehmer:innen überhaupt zulässig sein kann; bei richtiger Auslegung der einschlägigen datenschutzrechtlichen Bestimmungen ist aber davon auszugehen, dass **ohne wirksame Betriebsvereinbarung mit ausreichender Mitwirkung des Betriebsrates und im Einzelfall vorliegender berechtigter Interessen eine Durchsuchung der Konten ohne Zustimmung der Betroffenen wohl unzulässig ist.**

B. Tracking im Dienstfahrzeug

1. Sachverhalt

GPS-Tracking bietet eine Reihe an Möglichkeiten, Arbeitsabläufe zu optimieren und Verwaltungsaufwand zu sparen. So wurde bereits in der Vergangenheit von Arbeitgeber:innen vorgebracht, dass die GPS-Technik dem Schutz der Fahrzeuge, der monatlichen Abrechnung mit der Leasingfirma, der Routenplanung und -optimierung und vielem mehr diene. Nicht vergessen werden darf jedoch ein

[3]) Gem § 96 Abs 1 Z 3 ArbVG bedürfen Kontrollmaßnahmen, die die Menschenwürde der Arbeitnehmer:innen berühren, der Zustimmung des Betriebsrats in Form einer Betriebsvereinbarung. Eine Kompetenzübertragung gem § 114 Abs 1 ArbVG erfolgte im gegenständlichen Fall nicht, weshalb nicht der einbezogene Zentralbetriebsrat zuständig war und somit ein unzuständiges Organ die „Zustimmung erteilte".

[4]) Anzumerken ist an dieser Stelle, dass es sich bei der Beschwerdegegnerin um eine Körperschaft öffentlichen Rechts handelt, weshalb die Maßnahme bereits aufgrund der fehlenden gesetzlichen Grundlage unzulässig war.

[5]) Der Bescheid ist im Zeitpunkt der Drucklegung, soweit ersichtlich, noch nicht rechtskräftig.

[6]) DSB 13. 5. 2014, DSB-D600.328-001/0001-DSB/2014.

zweiter zentraler Aspekt: GPS-Tracking ermöglicht – gewollt oder ungewollt – die **minutiöse Überprüfung des Aufenthaltsorts der eigenen Arbeitnehmer:innen,** und damit, insbesondere bei Außendienstmitarbeiter:innen, eine engmaschige Kontrolle. Im gegenständlichen Fall wurde den Außendienstmitarbeiter:innen ein **Dienstfahrzeug** zur Verfügung gestellt, das mit einem **GPS-Tracker** versehen war. Für private Fahrten gab es die Möglichkeit, den Tracker zu deaktivieren.

2. Rechtliche Beurteilung

Völlig unstrittig stellt die Verwendung von GPS-Tracking eine Verarbeitung personenbezogener Daten gem Art 4 Z 1 DSGVO dar.[7]) Daraus folgt, dass ein Erlaubnistatbestand gem Art 6 Abs 1 DSGVO vorliegen muss: Bereits in einer vergangenen Entscheidung aus dem Jahr 2018 hatte sich die Datenschutzbehörde mit der Frage beschäftigt, **ob** es sich bei einer **Einwilligung** zur Nutzung von GPS im Rahmen eines Arbeitsverhältnisses um eine **freiwillige Zustimmung iSd Art 7 DSGVO** handelt.[8]) Die Freiwilligkeit der Zustimmung wurde im Rahmen des Arbeitsverhältnisses verneint; eine Prüfung nach Art 6 Abs 1 lit f DSGVO unterblieb im damaligen Beschwerdeverfahren.[9])

In der vorliegenden Entscheidung[10]) kam es nun auch zu einer Überprüfung, ob die Verwendung von GPS-Tracking nach **Art 6 Abs lit f DSGVO**[11]) gerechtfertigt sein könnte. Ein berechtigtes Interesse[12]) kann ohne weiters dargelegt werden, jedoch **verneinte** die DSB sowohl die **Erforderlichkeit** als auch die **Verhältnismäßigkeit** der Nutzung. Die DSB bringt im Wesentlichen vor, dass es auch gelindere Mittel gäbe, welche mit einem weitaus geringeren Ausmaß an Datenverarbeitung auskämen, um die vorgegebenen Ziele zu erreichen. Die Verwendung von GPS-Trackern bedingt eine derart umfassende Datenverarbeitung, welche nur im äußersten Ausnahmefall gerechtfertigt ist. Zu betonen ist, dass die DSB zu dieser rechtlichen Beurteilung gekommen ist, obwohl das GPS-Tracking für private Fahrten deaktiviert werden konnte. Daraus folgt, dass der Einsatz von GPS-Trackingtechnologie aus datenschutzrechtlicher Sicht **im betrieblichen Bereich,** wenn überhaupt, **nur äußerst eingeschränkt möglich** ist.[13])

---

[7]) *Jahnel*, Kommentar zur Datenschutz-Grundverordnung (DSGVO) (2020) Art 4 Rz 21.

[8]) Zu beachten ist der Umstand, dass § 10 Abs 1 AVRAG vorsieht, dass „[d]ie Einführung und Verwendung von Kontrollmaßnahmen und technischen Systemen, welche die Menschenwürde berühren", nur mit Zustimmung des Betriebsrats zulässig ist. Da im gegenständlichen Fall kein Betriebsrat existierte, wurde gem § 10 Abs 1 AVRAG letzter TS die (ungültige) Zustimmung der einzelnen Arbeitnehmer:innen eingeholt.

[9]) DSB 8. 8. 2018, D213.658/0003-DSB/2018; Newsletter der DSB 4/2018, S 3.

[10]) DSB 1. 3. 2022, 2021-0.789.408 (D124.3940), Newsletter der DSB 2/2022, S 5.

[11]) Da sich die Beschwerdegegnerin auch auf das AZG iVm Art 6 Abs lit c DSGVO stützte, stellte die DSB fest, dass eine alleinige Berufung auf das AZG keine ausreichende Rechtsgrundlage darstelle.

[12]) Beispielhaft: Schutz der Fahrzeuge, der monatlichen Abrechnung mit der Leasingfirma, der Routenplanung und -optimierung etc.

[13]) Der Bescheid ist im Zeitpunkt der Drucklegung, soweit ersichtlich, noch nicht rechtskräftig.

C. Kamera und Mikrofonzugriff am Arbeitshandy

1. Sachverhalt

Der Beschwerdeführer war sowohl einfacher Arbeitnehmer der Beschwerdegegnerin als auch Mitglied des Betriebsrats. Zur Vereinfachung der Berechnung der Provision (für verkaufte Produkte) der Arbeitnehmer:innen wurde mittels **Betriebsvereinbarung** die Nutzung sogenannter **„vPOS"-Geräte**[14]) vereinbart. Bei diesen Geräten handelte es sich um Handhelds, die einem Mobiltelefon vergleichbar sind. In der Betriebsvereinbarung wurden die Bedingungen für die Datenverarbeitung **im Detail festgelegt,** um die Sicherheit der Daten und der Privatsphäre der Belegschaft zu schützen. So wurden sowohl die Kategorien der regelmäßig verarbeiteten Daten als auch die erlaubten Zwecke klar umschrieben; eine Auswertung zur Leistungsbeurteilung wurde explizit ausgeschlossen. Insbesondere wurde festgehalten, dass **jede substanzielle Veränderung** der vereinbarten Verwendung der „vPOS"-Geräte eine **Anpassung der Betriebsvereinbarung** voraussetzt. Nach einigen Monaten Nutzungszeit der vPOS-Geräte durch die Belegschaft erschien lokal in der Applikation des vPOS-Geräts die digitale Aufforderung, der App „alle Berechtigungen zu gewähren". Die geforderte Berechtigung umfasste insbesondere auch einen **Zugriff auf die Kameras und die Mikrofone der Mobiltelefone** der Arbeitnehmer:innen. Eine Verwendung ohne die Erteilung dieser Einwilligung durch die jeweiligen Arbeitnehmer:in war nicht mehr oder nur mehr sehr eingeschränkt möglich.

Bereits die Aufforderung zu einer nicht in der Betriebsvereinbarung gedeckten Nutzung widerspricht den Grundsätzen der DSGVO, die jede Datenverarbeitung an das Prinzip der Rechtmäßigkeit bindet. Im gegenständlichen Fall kam jedoch verschärfend hinzu, dass der Beschwerdeführer seinen Vorgesetzten um Hilfe bat, die Aufforderung zu quittieren, um wieder ein gewohntes Arbeiten zu ermöglichen. Statt die rechtswidrige Aufforderung zu löschen, ordnete der Vorgesetzte eine **Fernfreischaltung der Kamera und des Mikrofons ohne Einwilligung** des Beschwerdeführers und des Betriebsrats an. Darüber hinaus stellte sich heraus, dass die Beschwerdegegnerin, entgegen der Betriebsvereinbarung, die Daten zur **Leistungsbeurteilung** verwendete.

2. Rechtliche Beurteilung

Gegen die massiven Eingriffe in die Privatsphäre hat der betroffene Mitarbeiter Beschwerde wegen Verletzung seines Rechts auf **Geheimhaltung** (§ 1 DSG), Verletzung der **Grundsätze der Datenverarbeitung** (Art 5 DSGVO) und **Fehlen eines Erlaubnistatbestands** (Art 6 DSGVO) an die DSB erhoben. Da eine Einwilligung gem Art 6 Abs 1 lit a DSGVO evidentermaßen nicht vorlag (die Betriebsvereinbarung sieht vor, dass kein Zugriff auf die Kamera und das Mikrofon stattfindet, eine Einzelzustimmung war nicht erteilt worden), kommt lediglich ein berechtigtes Interesse gem Art 6 Abs 1 lit f DSGVO, dem kein überwiegendes schutzwürdiges Interesse des Betroffenen gegenübersteht, als Rechtsgrundlage der Verarbeitung in Betracht: Die Berufung auf Art 6 Abs 1 lit f DSGVO schei-

[14]) Bei „vPOS"-Geräten handelt es sich um Online-Terminals für bargeldloses Bezahlen an einem bestimmten Verkaufsort.

tert aber bereits am „berechtigten Interesse", also auf der ersten Prüfstufe. **Die Beschwerdegegnerin konnte kein berechtigtes Interesse an der Verwendung der Kamera und des Mikrofons nachweisen.** Die DSB musste daher gar nicht mehr prüfen, ob die schutzwürdigen Interessen der Arbeitnehmer:innen, nicht optisch und akustisch überwacht werden zu können, ein berechtigtes Interesse der Arbeitgeberin übersteigen würden – was aber wohl der Fall gewesen wäre.

Das gegenständliche Vorgehen steht in eklatantem Widerspruch zu den Grundsätzen der DSGVO, derartige Eingriffe in die Privatsphäre sind in der Regel ausschließlich mittels Zustimmung durch Betriebsvereinbarung (§ 10 AVRAG) zu rechtfertigen. Sollte es keinen Betriebsrat geben, wäre eine Zustimmung durch die einzelnen Dienstnehmer:innen nach § 10 AVRAG denkbar; wie jedoch bereits weiter oben ausgeführt, muss diesfalls besonders darauf Bedacht genommen werden, die Freiwilligkeit gem Art 7 DSGVO zu wahren. Ob eine solche im gegenständlichen Fall möglich gewesen wäre, war nicht Gegenstand der Beschwerde. [15])

D. Arbeitszeitaufzeichnung mit Handvenenscanner

1. Sachverhalt

Im Fall **„Handvenenscanner"** hatte die Arbeitgeberin die originelle Idee, die Identifikation der Arbeitnehmer:innen bei Einsichtnahme in arbeitsrechtliche Unterlagen und insbesondere Bestätigung von Arbeitszeitaufzeichnungen mittels Handvenenscanner[16]) vorzunehmen. Dabei mussten die Arbeitnehmer:innen bereits im **Arbeitsvertrag** der Verarbeitung ihrer biometrischen Daten **zustimmen.** Vor der erstmaligen Ausführung des Handvenenscans war es möglich, diese Einwilligung datenschutzrechtlich zu widerrufen. Tatsächlich nutzten 23% der Arbeitnehmer:innen die Möglichkeit des Handvenenscans nicht, dies mit der Konsequenz, dass eine selbständige Einsicht in die Unterlagen nicht mehr möglich war, sondern nur nach Identifikation durch eine Mitarbeiter:in des Personalbüros. Sanktionen oder sonstige Auswirkungen hatte der Widerruf in der Praxis nach Angaben der Arbeitgeberin nicht. Festzuhalten ist aber, dass der nachträgliche, datenschutzrechtlich zulässige Widerruf der Einwilligung zivilrechtlich einen Verstoß gegen die im Arbeitsvertrag übernommenen Pflichten bedeutet.

---

[15]) DSB, D124.2507. Das Verfahren wurde auf Grundlage der klaren Rechtslage mittels Generalvergleich erledigt, weshalb die Beschwerde zurückgezogen wurde. Es liegt somit keine rechtskräftige Entscheidung vor.

[16]) Ein Handvenenscanner scannt die Venenmuster auf der Handinnenfläche oder auf dem Handrücken und versieht diese mit einem Hashwert, um so eine eindeutige Zuordnung zu ermöglichen. Die Venenstruktur bleibt zeitlebens unverändert und gewährt ein ähnlich hohes Sicherheitsniveau wie ein Irisscanner. Der klassische Anwendungsbereich solcher Geräte liegt in der Regel im Hochsicherheitsbereich zur Zutrittssicherung; die Speicherung derartiger biometrischer Identifizierungsmerkmale birgt aber auch ein hohes Risiko eines möglichen Identitätsdiebstahls.

2. Rechtliche Beurteilung

Die gegenständliche Entscheidung[17]) der Datenschutzbehörde beinhaltet eine Reihe bemerkenswerter Feststellungen zur Verwertung biometrischer Daten der Arbeitnehmer:innen:

Die Datenschutzbehörde erblickt in der gegenständlichen Verwendung des Handvenenscanners **keine Kontrollmaßnahme, die die Menschenwürde berührt.** Demnach sind auch die Bestimmungen des § 10 AVRAG iVm § 96 Abs 1 Z 3 ArbVG nicht anwendbar. Eine Zustimmung des Betriebsrats bzw bei dessen Fehlen der betroffenen Arbeitnehmer:innen ist daher zum Einsatz des Systems, das lediglich die Identifikation der Arbeitnehmer:innen und deren Zustimmung bei der Einsicht in sie betreffende Unterlagen in Zusammenhang mit dem Dienstverhältnis ermöglicht, nicht zwingend notwendig. Zwar stellt der Scan der Handvenen einen tiefen Eingriff in die Privatsphäre der Arbeitnehmer:innen dar, jedoch handelt es sich in der von der Beschwerdegegnerin genutzten Art **nicht um ein Kontrollsystem.** Das System wurde vielmehr verwendet, um nicht einen gesonderten Identitätsnachweis bei der Einsicht in die Unterlagen durchführen zu müssen. Allerdings sind die Besonderheiten des **arbeitsrechtlichen Druckverhältnisses** für die Beurteilung der **datenschutzrechtlichen Freiwilligkeit** der Zustimmung von besonderer Bedeutung.

Unbestritten stellt ein Handvenenscan und die damit verbundene Erstellung eines einzigartigen Hashwerts zur Wiedererkennung der gescannten Hand eine Verarbeitung personenbezogener Daten iSd der Art 4 Z 1 und Z 2 DSGVO dar. Dabei handelt es sich um **biometrische Daten iSd Art 4 Z 14 DSGVO.** Die Einwendungen der Beschwerdegegnerin, dass lediglich der Hashwert gespeichert wird und somit keine Verarbeitung von biometrischen und somit besonders schützenswerten Daten erfolgt sei, wurde richtigerweise zurückgewiesen. Jeder Scan für sich stellt bereits eine Verarbeitung iSd Art 4 Z 2 DSGVO dar, selbst wenn anschließend lediglich ein Hashwert gespeichert wird.

Da es sich bei biometrischen Daten um sogenannte **„besonders schutzwürdige Daten"** (nach alter Rechtslage: „sensible Daten") handelt, bedarf es zur (grundsätzlich verbotenen) Verarbeitung eines besonderen Erlaubnistatbestands nach Art 9 Abs 2 DSGVO. Der taxative Katalog an Erlaubnistatbestände lässt im gegenständlichen Fall **ausschließlich** eine Berufung auf die **ausdrückliche Einwilligung** zu einem bestimmten Verarbeitungszweck zu.

Wie auch bei der Einwilligung nach Art 6 Abs 1 lit a DSGVO muss bei der Einwilligung nach Art 9 Abs 2 DSGVO aber das **Kriterium der Freiwilligkeit** gem Art 7 DSGVO iVm Art 4 Z 11 DSGVO iVm dem ErwGr 43 DSGVO vorliegen. Dabei gilt nach der DSGVO, dass eine Einwilligung nur freiwillig ist, wenn die betroffene Person eine echte Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden (Art 4 DSGVO). Keine Freiwilligkeit liegt vor, „wenn zwischen der betroffenen Person und der Verantwortlichen ein klares Ungleichgewicht besteht" (ErwGr 43 zur DSGVO). Eine Einwilligung darf auch nicht an die Erfüllung eines Vertrags gekoppelt sein

[17]) DSB 19. 10. 2022, DSB-D124.2941/2022-0.360.359; Newsletter der DSB 1/2023, S 4.

(Koppelungsverbot), auch in einem solchen Fall ist die Freiwilligkeit jedenfalls ausgeschlossen. Sollte also schon der Abschluss eines Arbeitsvertrags an die Zustimmung zur Verarbeitung biometrischer Daten gekoppelt sein, handelt es sich somit um eine ungültige Zustimmung.

Im vorliegenden Fall waren für die Beurteilung die Leitlinien 5/2020 des Europäischen Datenschutzausschuss (EDSA) zum Themenkomplex der Freiwilligkeit das zentrale Argument. Der Leitfaden, der als Interpretationshilfe der DSGVO gilt, führt folgende Kriterien an, die die Freiwilligkeit ausschließen können:

- **Ungleichgewicht der Macht,**
- Konditionalität,
- Granularität und
- Nachteil.

Der EDSA geht zur Frage des Machtungleichgewichts davon aus, dass bei einem **offenkundigen Ungleichgewicht der Macht** – wobei Arbeitsverhältnisse als Prototyp eines solchen Ungleichgewichts gesehen werden können[18]) – eine **rechtskonforme Einwilligung nur schwer nachzuweisen sein wird.** Er lehnt bei der Verarbeitung personenbezogener Daten im arbeitsrechtlichen Kontext das **Kriterium der Freiwilligkeit generell ab,** weil aufgrund der besonderen Drucksituation eine solche in der Regel nicht gegeben sein wird. Dies muss insbesondere für die Verarbeitung sensibler Daten gem Art 9 Abs 1 DSGVO gelten.

So entschied die Datenschutzbehörde richtigerweise, dass die **Zustimmung im Arbeitsvertrag datenschutzrechtlich unwirksam** war, da dort kein Hinweis auf die Freiwilligkeit und Widerruflichkeit der Zustimmung gegeben war. Aber auch die Aufklärung über die Freiwilligkeit und jederzeitige Widerruflichkeit im Rahmen der erstmaligen Durchführung des Handvenenscans war datenschutzrechtlich nicht ausreichend, weil die Arbeitnehmer:innen dabei die arbeitsvertraglich gegebene Zustimmung verletzen musste und ihm dies im Verhältnis zur Arbeitgeberin – ungeachtet der Frage, ob dies arbeitsrechtlich sanktionierbar gewesen wäre, nicht als freiwillige Wahl zuzumuten war.

Allgemein kann aus dieser Entscheidungspraxis der DSB für den Bereich des Arbeitsrechts der Schluss gezogen werden, dass eine auf die Einwilligung der Arbeitnehmer:innen gestützte Datenverarbeitung nur in absoluten Ausnahmefällen als tauglicher Erlaubnistatbestand in Frage kommen kann, weil aufgrund der besonderen Drucksituation die **Freiwilligkeit in der Regel verneint wird**.[19])

E. Videoüberwachung am Arbeitsplatz

1. Sachverhalt

Dieselbe Arbeitgeberin, welche auch die Handvenenscanner zum Einsatz brachte, verwendete zur Überwachung ihres (überschaubaren) Betriebs 29 Videokameras. Die Videokameras dienten nach unbestrittener Feststellung der Kontrolle, ob es bei der Entsorgung bzw der Anlieferung zu Beschädigungen oder

[18]) EDSA: Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 Rz 21; auffindbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.

[19]) Der Bescheid ist im Zeitpunkt der Drucklegung noch nicht rechtskräftig.

Diebstählen kam. **Eine gezielte Überwachung der Arbeitnehmer:innen der Beschwerdegegnerin war damit nicht verbunden.** Die aufgezeichneten Bilddaten wurden nach 72 Stunden automatisiert und ungesehen vernichtet, sofern nicht ein besonderes Ereignis (Einbruch, Beschädigung) Anlass zur Überprüfung der Materialien bot. Auf die Videoüberwachung wurde sowohl im Eingangsbereich als auch auf der Webseite hingewiesen. Festzuhalten ist auch, dass die Arbeitnehmer:innen und so auch der Beschwerdeführer nur fallweise und nie durchgehend im Aufnahmebereich der Videokameras arbeiteten. Die Videokameras waren von der Datenschutzbehörde auf der Grundlage des alten Datenschutzgesetzes 2000 registriert worden; die Behörde hatte damals keine Einwände.

2. Rechtliche Beurteilung[20])

Die Aufzeichnung mittels Videokamera stellt eine Verarbeitung personenbezogener Daten gem Art 4 Z 2 DSGVO dar. Dabei ist unbeachtlich, wie lange die Daten gespeichert werden und ob sie tatsächlich von einer natürlichen Person analysiert werden – **die Speicherung allein stellt bereits eine Verarbeitung dar** und bedarf des Vorliegens eines Erlaubnistatbestands. Da die Videoüberwachung im Wesentlichen der Kontrolle der Anlieferung und Entsorgung dienen sollte, **verneinte** die Datenschutzbehörde das **Vorliegen einer Kontrollmaßnahme,** die auf die Kontrolle der Arbeitnehmer:innen gerichtet ist. Dies hat aus datenschutzrechtlicher Sicht zwei gravierende Auswirkungen:

Erstens war es so der Arbeitgeberin weiterhin möglich sich auf Art 6 Abs 1 lit f DSGVO zu stützen und es war keine zwingende Einwilligung der Arbeitnehmer:innen gem § 10 AVRAG notwendig (im Betrieb war kein Betriebsrat eingerichtet). Zweitens sind gem § 12 Abs 4 DSG **Bildaufnahmen** zum **Zweck der Kontrolle von Arbeitnehmer:innen absolut unzulässig.**[21])

Auch wenn es zu keiner gezielten Kontrolle der Arbeitnehmer:innen durch die Videoüberwachung gekommen ist, sind die Wertungen des Gesetzgebers, dass im Rahmen eines Beschäftigungsverhältnisses eine Videoüberwachung, wenn auch nur beiläufig, einen **besonders schweren Privatrechtseingriff** darstellt, zu beachten. Im vorliegenden Fall hatte sich der Beschwerdeführer idR nur am Rande und nur zeitweise im Aufnahmefeld der Videokamera befunden – eine durchgehende Aufnahme, welcher sich der Arbeitnehmer gar nicht oder nur schwer entziehen könnte, wäre strenger zu bewerten, weil darin jedenfalls ein Eingriff in die höchstpersönliche Sphäre vorläge.

Die Entscheidung der DSB in dieser Causa fällt **differenziert** aus: So ist auch im Rahmen des Arbeitsverhältnisses eine Überwachung mittels Bildaufnahmen zulässig – jedoch selbstverständlich nie zur Überwachung der Arbeitnehmer:innen. Der Schutz des Eigentums oder auch der Schutz von Gästen stellt ein berechtigtes Interesse gem Art 6 Abs 1 lit f DSGVO dar. Jedoch muss stets genau geprüft

[20]) GZ: DSB-D124.2941/2022-0.360.359.

[21]) Nach der Judikatur des BVwG sind §§ 12 und 13 DSG mangels entsprechender Öffnungsklausel in der DSGVO nicht anwendbar. Dies ändert nach Auffassung der DSB im zitierten Bescheid jedoch nichts daran, dass der einschränkende § 12 Abs 4 DSG weiterhin anwendbar bleibt und Bildaufnahmen zur Kontrolle von Arbeitnehmer:innen absolut unzulässig bleiben.